Fırat Üniv. Müh. Bil. Dergisi
29(2), 15-21, 2017

Science and Eng. J of Fırat Univ.
29(2), 15-21, 2017

LFSR Soru Girdisi İle PUF Tasarımının Gerçeklenmesi

Erdinç Avaroğlu
Mersin Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Mersin
eavaroglu@mersin.edu.tr

(Geliş/Received: 05.11.2016; Kabul/Accepted: 14.06.2017)

Özet

PUF'lar, tüm devre üretimi sırasındaki kontrol edilemeyen süreçlere dayalı olarak her bir yongaya özgü imza üreten tümdevre bileşenleridir. PUF tasarımları soru-cevap (challange-response) ilişkisine bağlıdır. Sisteme verilen sorulara bağlı olarak cevaplar üretilir. Üretilen cevapların rasgeliliği sisteme verilen sorulara bağlıdır. Cevapların rasgeliliğini arttırmak amacıyla makalede, LFSR'den üretilen sayılar PUF'un girişlerine soru olarak verilmiştir ve kaotik işaret verilerek üretilen cevaplar ile karşılaştırılmıştır. RO tabanlı PUF tasarımı FPGA ortamında gerçekleştirilmiştir. Elde edilen cevapların istatistiksel özellikleri incelenmiş olup sonuçlar verilmiştir.

Anahtar kelimeler: PUF, Soru-cevap mekanizması, İstatistiksel testler, Ölçek indeks.

Implementation of PUF Design with LFSR Question Input

Abstract

Physically unclonable functions – PUFs are all circuits components. During the production of all circuit, based on process can not be controlled, they produce unique signature for each chip. The PUF designs depend on the challange-response relationship. Responses are generated depending on the challanges given to the system. In order to increase the randomness of response, Numbers generated from the LFSR are given as inputs to the PUF's challanges and compared with the responses generated by chaotic sign. The RO-based PUF design was implemented in an FPGA environment. Statistical properties of the resulting answer has been examined and successful results has been obtained.

Keywords: PUF, Challange-response mechanism, Statistical test, Scale index

1. Giriş

Rasgele sayılar, belirli bir aralık için tanımlanmış, oluşma olasılıkları birbirine eşit ve bu sayılar arasında belirli bir ilişki olmayan sayılar olarak tanımlanabilir. Rasgele sayılar simülasyon, örnekleme, nümerik analiz, karar verme, eğlence, bilgisayar programlama ve kriptografi alanlarında çokça kullanılmıştır. Rasgele sayıların aşağıda belirtilen şu özellikleri sağlaması gerekmektedir:

- Tahmin edilememe
- Tekrar Üretilememe (aperiyodiklik)
- İyi istatistiksel özellikler
- Düzgün dağılım

Rasgele sayıları elde etmek amacıyla sözde rasgele sayı üreteçleri (SRSÜ) ve gerçek rasgele sayı üreteçleri (GRSÜ) olmak üzere çeşitli sayı üreteçleri geliştirilmiştir. Sözde rasgele sayı üreteçleri herhangi bir başlangıç (tohum) değeri ile belirli bir algoritmaya tabi tutularak uzun rasgele sayı dizileri üretmişlerdir. Gerçek rasgele sayı üreteçleri gürültü kaynağı olarak gerçek fiziksel süreçleri kullanarak rasgele sayı üretirler [1]. Bu iki üreteçten özellikle gerçek rasgeleliği ve güvenliği sağlaması nedeniyle donanım tabanlı gerçek rasgele sayı üreteçleri kullanılmaktadır[1]. Ancak son yıllarda bu donanımların (cihazların) fiziksel saldırılara karşı savunmasız olduğu kanısı ortaya atılmıştır [2]. Bu nedenle bu tarz sorunların giderilmesi için PUF'lar kullanılmıştır. PUF'lar belirli bir donanıma bağlı olan rasgele fonksiyonlardır. PUF'u, daha güvenlikli kriptografik protokollere gizli anahtar sağlanması amacıyla kullanmak mümkündür.

Genel olarak PUF, bir fiziksel materyalin karmaşık ve değişken doğasına bağımlı olarak tutulan cevap ve soru arasındaki haritalamaya dayanan bir soru-cevap mekanizmasıdır. PUF, Şekil 1'de görüldüğü üzere m-bit soruyu alır ve n-bit cevap üretir.

Şekil 1. Genel PUF tasarımı

Eğer puf devresi farklı chipler üzerinde gerçekleştirilirse, her bir PUF aynı soru (C) girildiğinde bile benzersiz cevaplar (R) üretir.

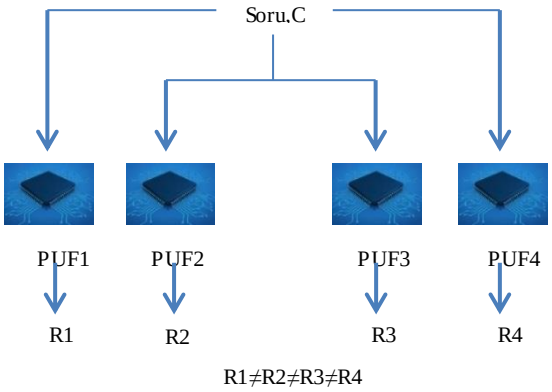
Literatürde PUF tasarımları, elektronik ve elektronik olmayan olmak üzere 2 ana grup altında toplanmaktadır. Elektronik PUF'larda, soru-cevap mekanizması kapı gecikmeleri, transistörün eşik gerilimi gibi elektronik özelliklerine göre belirlenir. Arbiter PUF, Ring Oscillator PUF, SRAM PUF ve Butterfly PUF gibi çeşitli elektronik PUF tasarımları bulunmaktadır [3–6]. Elektronik olmayan PUF'larda ise soru-cevap mekanizması elektronik olmayan ışık ve ses gibi özellikler ile belirlenir. Optical PUF ve Acoustical PUF gibi tasarımlarda elektronik olamayan PUF tasarımlarıdır [7,8].

PUF'lar eşsizlik, kopyalanamama ve tahmin edilememe gibi temel özellikleri ile birçok güvenlik gereksinimini sağlıyorken tersine mühendislik, emülasyon ve ortadaki adam saldırısı gibi saldırılara maruz kalmaktadır. Bu amaçla önerilen sistemde, elde edilecek cevapların rasgeliliğini arttırmak ve PUF'un maruz kalacağı saldırıların önüne geçmek amacıyla x^2+x+1 karakteristik denklemine sahip LFSR yapısı soru olarak verilmiştir. Gerçekleştirilen RO tabanlı PUF devresinde her biri 3 Inverterden oluşan 128 RO kullanılmıştır. Sistemden elde edilen cevaplar bir hafıza devresine kaydedilmiştir. Elde edilen sonuçlar [9]'da yapılan çalışmada soru olarak kullanılan kaotik işaret ile karşılaştırılmıştır. Ayrıca bu cevapların kriptografide kullanılabilirliğini göstermek için istatistiksel test (NIST), ölçek index (scale index), istatistiksel karmaşıklık ölçüsü (statistical complexity measure (SCM)) ve oto korelasyon test sonuçları elde edilmiştir.

Makalenin geri kalan kısmı aşağıdaki gibi organize edilmiştir. 2. Bölümde PUF devrelerinin temel özellikleri verilmiştir. 3. Bölümde önerilen sistemin yapısı ve gerçekleştirilmesi sunulmuştur. 4. Bölümde istatistiksel test (NIST), ölçek index, SCM ve oto korelasyon açıklamaları ve elde edilen sonuçlar verilmiştir. Son bölümde sonuçlar tartışılmıştır.

2. Fiziksel Klonlanamaz Fonksiyonlar

PUF, Şekil 3 'te görüldüğü üzere bir fiziksel materyalin karmaşık ve değişken doğasına bağımlı sisteme girilen m bit challage ile eşsiz n-bit responselar üretebilen bir yapıya sahiptir.



Şekil 2. Genel PUF tasarımının çalışma prensibi

Burada, C her biri ile m-bit ikili giriştir. R1,R2,R3 ve R4 cevaplarıda n bit ikili dizidir.

PUF'ların eşsizlik, kopyalanamama ve tahmin edilememe gibi temel özellikleri mevcuttur. Eşsizlik özelliği, bir PUF'un farklı devreler üzerinde aynı sorular ile farklı cevaplar üretmesidir. PUF'un en temel özelliği olan kopyalanamama ise birbirinin aynı iki devrenin yapılmasının mümkün olmadığı anlamına gelmektedir. Bir diğer en önemli özellik ise PUF cevaplarının tahmin edilemez olmasıdır. PUF'un bu kaliteli özelliklerinden dolayı kimlik doğrulama, kriptografik anahtar üretimi ve fikri mülkiyet koruma gibi uygulamalar için gelecek vaat eden bir çözüm haline gelmiştir. PUF'lar bu temel özellikleri ile birçok güvenlik gereksinimi sağlarken tersine mühendislik, emulasyon ve ortadaki adam saldırıları gibi güvenlik açıklarından muzdarip olabilirler [10]. Tersine mühendislik saldırıları ile PUF klonlanmaya çalışılmaktadır. Emulasyon saldırıları, tüm olası soru-cevap çiftlerini (CRP) depolamaya çalışır. Ortadaki adam saldırıları, PUF ve kimlik doğrulama sunucusu arasındaki CRP bilgi değişimini çalmak ister.

Bu güvenlik açıklarının önüne geçilmesi amacıyla oldukça büyük cevaplar elde etmek gereklidir. Çünkü;

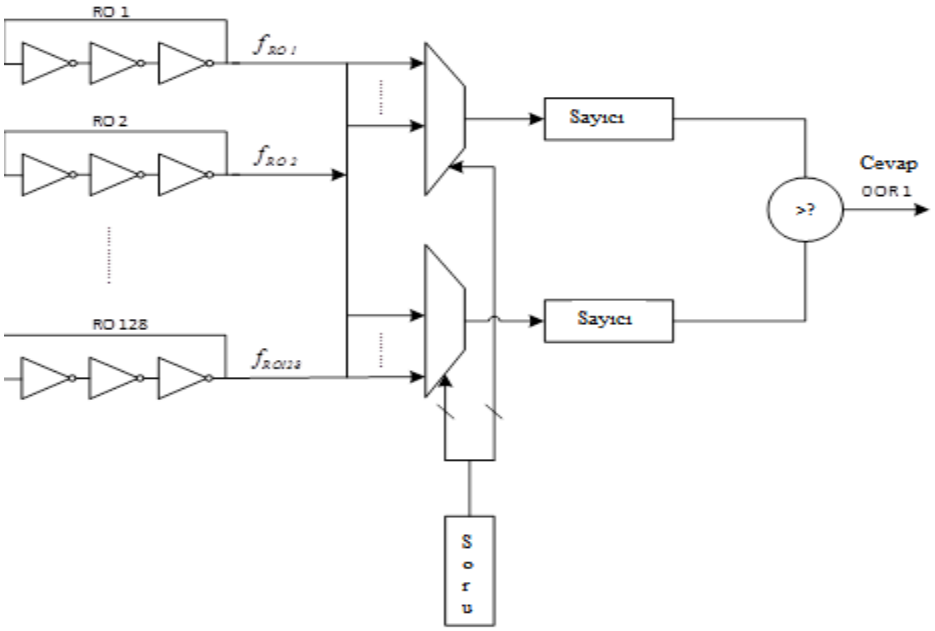
1. PUF cevaplarının büyük kümesi uzun şifreleme anahtarlarına yol açar, ki güçlü şifreleme sunabilir.
2. Bir cihaz kimlik doğrulama sürecinde, PUF CRPs cihaz kimlik doğrulaması ve kimlik doğrulama makamı arasında değiştirilebilir(değiş tokuş yapılabilir). Çünkü CRPs genel bilgidir ve transfer işlemi güvenli olmayan bir kanal üzerinden gerçekleşmesi nedeniyle bir saldırgan bu bilgiyi yakalayabilir ve değiştirebilir. Bu gibi tekrar saldırılarının önüne geçmek amacıyla CRP bir kereden fazla kullanılmamalıdır. Ancak bu büyük CRP kümeleri oluşturmayı gerektirir.
3. PUF'lar çevresel değişiklikler ve gürültü etkilerinden dolayı hatalı veya kararsız oldukları için PUF cevap bitlerinin sayısı güvenilir biçimde kullanılamaz. Bu hatayı telafi etmek için ek cevap üretmek gerekir.

Büyük cevaplar elde etmek için rasgele seçilen sorular kullanılmalıdır. Önerilen sistemde doğrusal olmayan LFSR soru yapısı kullanılarak cevap üretimi gerçekleştirilmiştir.

3. Önerilen Sistemin Yapısı ve Gerçekleştirilmesi

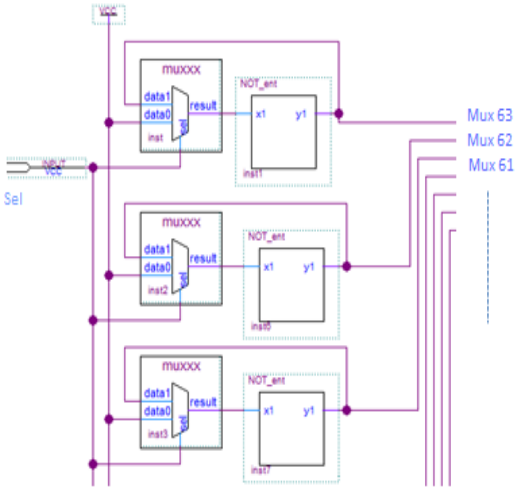
RO'lerin FPGA'de uygulanmasının kolay olması ve TRNG sistemlerinde kullanılan RO tabanlı rasgele sayı üreteçleri ile entegre edilebilmesi nedeniyle önerilen sistem Altera'nın EP4CE115F29C7 tabanlı FPGA bordunda gerçekleştirilmiştir.

Şekil 3'te genel RO tabanlı PUF tasarımı verilmiştir. Bu tasarımda her biri 3 inverter içeren 128 RO kullanılmıştır. RO lerin çıktıları 64x1 'lik birer Mux devresine giriş olarak verilmiştir. Sistemde kullanılan her bir RO VHDL dili ile dataflow ve şematik tasarım yöntemleri kullanılarak gerçekleştirilmiştir.



Şekil 3. Genel RO tabanlı PUF Tasarımı

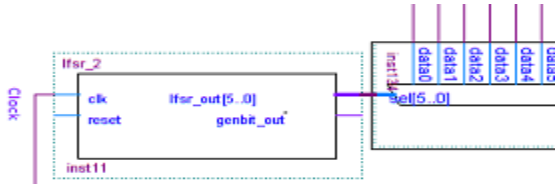
Şekil 4'te RO yapısını göstermektedir. Şekil 4'te inverter çıkışı sürekli olarak logic 0 seviyesindedir. RO tarafından rasgele işaretin elde edilmesi için fiziki ortamdan bir uyartım işaretinin (sel=1) verilmesi ile RO çıkışı elde edilmektedir.



Şekil 4. RO tasarımı

Herbir RO'den elde edilen çıkışlar birer mux devresine girilmektedir. Mux devresine giriş olarak verilen RO'lerden hangisinin çıkışa aktarılacağı soru tarafından belirlenmektedir. Her bir MUX çıkışı bir sayıcıya girilerek sayıcıların ileri doğru sayması gerçekleştirilmektedir.

Bu makalede doğrusal olmayan 6 bitlik LFSR yapısı kullanılarak Soru devreleri gerçekleştirilmiştir. Kullanılan LFSR x2+x+1 karakteristik denklemine sahiptir. Sayıcılardan frekansı büyük olan cevap (Rasgele sayı) olarak kullanıldı. Elde edilen her bir rasgele sayının istatistiksel testlerini gerçekleştirmek hafıza birimine 50 mHz'lik örnekleme ile kaydedilmiştir. Hafıza 1 er bitlik değer saklayabilen 65535 adresten oluşmaktadır. Sayının hangi adrese kaydedileceğini belirlemek için ileri sayan bir sayıcı kullanılmıştır. Kullanılan LFSR x^2+x+1 karakteristik denklemine sahip olup Şekil 5'de gösterilmiştir.



Şekil 5. LFSR soru

[9]'da yapılan çalışmada ise, logistik harita tarafından rasgele soru işaretleri üretilmesi için floting point sayi sisteminde işlem yapabilen çarpma, çıkarma devreleri kullanılmıştır. Logistik haritanın sistem parametresi $r=3.99$ tohum değeri $X_0 = 0.2$ seçilmiştir. Üretilen bu sayıların 0.5'ten büyük olması durumunda 1 aksi durumda 0 sayısı üretilmiştir. Bu sayılara karşılık üretilen bit dizisi $1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0$ ... olmuştur. Logistik haritadan üretilen her 6 sayı {110000, 110011, 110010, … } soru girişlerine verilmiştir.

4. Deneysel Sonuçlar

Sistemden üretilen cevaplar kriptografik sistemlerde anahtar üretimi için gerekli olan rasgele sayı olarak kullanılacaktır. Elde edilen cevap'ların rasgeliliğini arttırmak için 6 bitlik LFSR sisteme soru olarak verilmiştir. Soru olarak kullanılan LFSR ile [9]'da soru olarak kullanılan kaotik işaret ile karşılaştırılmıştır. Ayrıca önerilen sistemin kriptografik uygulamalarda güvenli olarak kullanılabilmesi için rasgelelik testlerine tabi tutulması gerekmektedir. Üretilen sayıların rasgeleliğini analiz etmek için birçok test suiti geliştirilmiştir. Bunların başlıcaları NIST istatistiksel test, SCM ve oto korelasyon testleri olup elde edilen sonuçlar aşağıda verilmiştir.

4.1. NIST istatistiksel test

Rasgele sayı üreteçleri tarafından üretilen uzun ikili bit dizilerinin rasgeleliğini ölçmek için geliştirilmiştir. 16 test içeren istatistiksel bir pakettir. Bu testler dizi içerisindeki rasgele olmayan durumlara odaklanır [11]. NIST 800.22 test suitine göre istatistiki test sonuçları aşağıdaki Tablo 1'de verilmiştir.

Tablo 1. Önerilen RO-PUF sisteminden elde edilen rasgele sayıların istatistiki test sonuçları

Test	LFSR	Lojistik Harita	Sonuç
Frekans	0.254	0.757	Başarılı
Blok Frekans Test	0.999	0.135	Başarılı
Akış Test	0.026	0.801	Başarılı
En Uzun Birler Test	0.106	0.497	Başarılı
İkili Matris RankıTest	0.707	0.336	Başarılı
Ayrık Fourier Test	0.350	0.501	Başarılı
Örtüşmeyen Şablon Eşleştirme Testi	0.213	0.698	Başarılı
Örtüşen Şablon Eşleştirme Testi	0.044	0.630	Başarılı
Maurer Test	0.300	0.435	Başarılı
Doğrusal Karmaşıklık Test	0.097	0.644	Başarılı
Seri Test	0.365	0.444 0.617	Başarılı
Yaklaşık Entropi Test	0.130	0.949	Başarılı
Kümlatif Toplam Test	0.500	0.880	Başarılı

4.2. Ölçek index yöntemi

Bir sinyalin veya üretilen sayı dizilerinin non-periyodiklik derecesi hakkında bilgi edinmemizi sağlayan scale index tekniği Benitez tarafından önerilmiştir [12].Kullanılan teknik, Sürekli Dalgacık Dönüşümü (Continous Wavelet Transform-CWT) ve dalgacık çoklu çözünürlük (wavelet multi resolution) analizine dayanmaktadır. Sistemin periyodiklik derecesini belirlemek için kullanılan yöntem aşağıda verilmiştir [13]. Ölçek s ve u zamanındaki f'in Sürekli Dalgacık Dönüşümü (CWT) ve scalogram Denklem 1 ve 2'teki gibidir.

$$Wf(u,s) \coloneqq \langle f, \psi_{u,s} \rangle = \int_{-\infty}^{+\infty} f(t)\psi_{u,s}^{*}(t)dt \quad (1)$$

$$S(s) \coloneqq \|Wf(u,s)\| = \left(\int_{-\infty}^{+\infty} |Wf(u,s)|^2 du\right) \quad (2)$$

S(s) bir scale s'deki f'in Sürekli Dalgacık Dönüşümünün enerjisidir. Bir ölçek s'deki f'in innerscalogramı denklem 3'deki gibidir.

$$S^{inner}(s) \coloneqq \|Wf(u,s)\|_{j(s)} = \left(\int_{c(s)}^{d(s)} |Wf(u,s)|^2 du\right)^2 \quad (3)$$

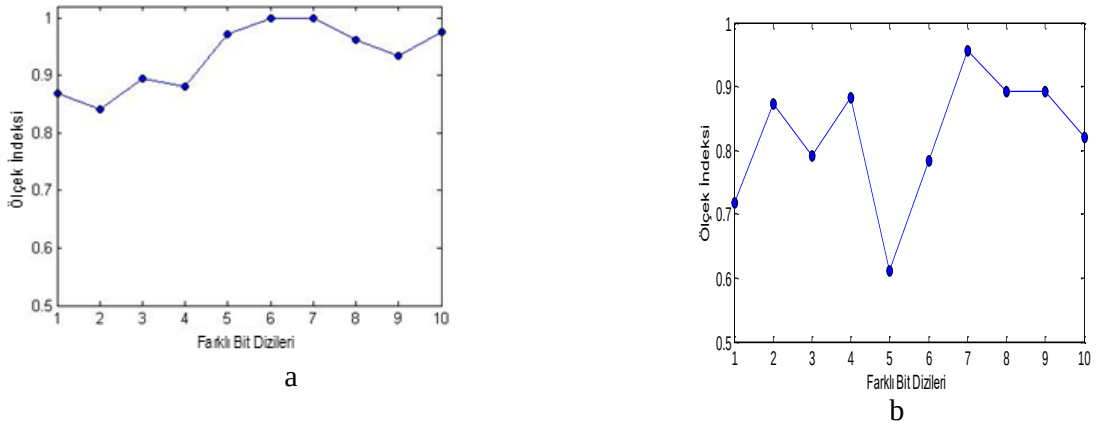
$J(s) = [c(s), d(s)] \subseteq I$, I'da maksimum alt aralığı göstermektedir. $\psi_{u,s}$'nin katkısı tüm u ϵ j(s) için I'da yer alır. J (s) in uzunluğu ile ilgili olarak, ölçek s'e bağlıdır, böylece farklı ölçeklerde iç scalogram değerleri karşılaştırılamaz. Normalize edilmiş s^{inner} denklem 4'deki gibidir.

$$\bar{S}^{inner}(s) = \frac{S^{inner}(s)}{(d(s)-c(s))^{\frac{1}{2}}} \quad (4)$$

[s0,s1] aralığındaki f'in ölçek indeksi denklem 5'deki gibidir.

$$i_{scale} \coloneqq \frac{S(s_{min})}{S(s_{max})} \quad (5)$$

Ölçek indeks değeri i_{scale}; $0 \leq i_{scale} \leq 1$ aralığında olmalıdır. Üretilen sistemden elde edilen i_{scale} değeri 0 veya 0'a yakın olursa sistem periyodik, 1 veya 1'e yakın olursa sistem non-periyodik olacaktır. Şekil6a.'da lojistik harita ve Şekil6b.'de ise LFSR'den elde edilen cevapların ölçek indeks sonuçları verilmiştir.



Şekil 6. a) Lojistik harita **b)** LFSR

4.3. Oto korelasyon test

Korelasyon, iki yada daha fazla değişken arasındaki doğrusal ilişkiyi gösterir.+1 ve -1 arasında değer alır. Eğer 0 veya 0 a yakınsa bu değişkenler arasında doğrusal ilişki yoktur. Bu testin amacı da üretilen bit dizisi bi ile onun kaydırılmış versiyonu arasındaki korelasyonu kontrol etmektir. d değerini sabit tamsayı ve 1≤d≤(n/2) olarak alalım. Testin matematiksel tanımlamaları Denklem 6 ve 7'de verilmiştir [14].

$$A(d) = \sum_{i=0}^{n-d-1} b_i \oplus b_{i+d} \quad (6)$$

Burada ⊕ XOR operatörü ve n bit dizisi uzunluğudur. Denklem 7'de tanımlanmıştır.

$$X_5 = \frac{2[A(d)-(n-d)/2]}{\sqrt{n-d}} \quad (7)$$

Eğer $\{b_i\}$ gerçek rasgele dizi ve $n \to \infty$ ise, bu rasgele değişken normal dağılıma N(0,1) sahiptir. α=0.05 alarak, eğer |X5|<1.6449 ise test başarılıdır [14]. Önerilen PRNG sisteminden elde edilen korelasyon test sonuçları Tablo 2'de verilmiştir.

Tablo 2. Oto korelasyon test sonuçları

	d	LFSR	Lojistik Harita	Sonuç
Oto Korelasyon	8	1.156	0.776	Başarılı
	10	0.572	1.300	Başarılı
	13	0.652	0.560	Başarılı

5. Sonuç

Bu çalışmada, RO PUF tasarımından elde edilen cevap'ların rasgeliliğini arttırmak ve PUF'un maruz kalacağı saldırıların önüne geçmek amacıyla non-periyodik yapıya sahip LFSR'den elde edilen soru yapısı kullanıldı ve kaotik işaret kullanılan soru yapısıyla karşılaştırma işlemi yapıldı. Her iki sistemden elde edilen cevapların NIST testlerinin tamamını başarı ile geçtiği ve otokorelasyon sonuçlarında başarılı olduğu gözlemlenmiştir. Ancak ölçek indeks yöntemi sonuçlarına bakıldığında soru olarak kaotik işaretler kullanılarak elde edilen cevapların daha periyodik olduğu gözlemlenmiştir. Önerilen sistemde üretilen rasgele sayılar en az sayıda inverter (3 inverter) içeren 128 RO ile PUF tasarımı gerçekleştirilmiştir. Sonuçlar herhangi bir son işleme tabi tutulmadan istatistiki testleri başarı ile geçmiştir. Sonuç olarak, elde edilen tüm test sonuçları değerlendirildiğinde önerilen sistemin de kriptografik sistemlerde güvenli anahtar üretiminde kullanılabileceği gösterilmiştir.

6. Kaynaklar

1. Koç, Ç. K. (2009). About Cryptographic Engineering, in Cryptographic Engineering, Ed. Springer US, 1–4.

2. Lee, J. W., Lim, D., Gassend, B., Suh, G. E., van Dijk, M. and Devadas, S. (2004). A technique to build a secret key in integrated circuits for identification and authentication applications, in 2004 Symposium on VLSI Circuits, Digest of Technical Papers, 176–179.

3. Gassend, B. (2003). Physical Random Functions, Master, MIT, MA,USA
4. Guajardo, J., Kumar, S. S., Schrijen, G.-J. and Tuyls, P. (2007). FPGA Intrinsic PUFs and Their Use for IP Protection, in Cryptographic Hardware and Embedded Systems - CHES 2007, P. Paillier and I. Verbauwhede, Eds. Springer Berlin Heidelberg, 63–80.
5. Kumar, S. S., Guajardo, J., Maes, R. , Schrijen, G.-J. and Tuyls, P. (2008). Extended abstract: The butterfly PUF protecting IP on every FPGA, in IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2008, 67–70.
6. Pappu, R. S. (2001). Physical one-way functions, Phd., Massachusetts Institute of Technology.
7. Pappu, R., Recht, B. , Taylor, J. and Gershenfeld, N. (2002). Physical One-Way Functions, Science, vol. 297, no. 5589, 2026–2030
8. Vrijaldenhoven, S., (2004) Acoustical Physical Uncloneable Functions, Master, Department of Mathematics and Computing Science ,Technische Universiteit Eindhoven.
9. Tuncer, T. (2016). The implementation of chaos-based PUF designs in field programmable gate array, Nonlinear Dyn., vol. 86, no. 2, 975–986
10. Majzoobi, M., Koushanfar, F. and Potkonjak, M. (2009). Techniques for Design and Implementation of Secure Reconfigurable PUFs, ACM Trans Reconfigurable Technol Syst, vol. 2, no. 1, 5:1–5:33
11. Rukhin, A., Soto, J., Nechvatal, J., Smid, M. and Banks, D. (2001). A statistical test suite for random and pseudorandom number generators for statistical applications, NIST Spec. Publ. Comput. Secur.
12. Benítez, R., Bolós, V. J. and Ramírez, M. E. (2010). A wavelet-based tool for studying non-periodicity, Comput. Math. Appl., vol. 60, no. 3,634–641
13. Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.-C. and Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map, Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 1, 101–111
14. Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A. (1996). Handbook of Applied Cryptography, 1 edition. Boca Raton: CRC Press